IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
SEATTLE DIVISION

DANIEL LOVELL, individually and on behalf of a class of those similarly situated,	)	No. _____
Plaintiff,	)	CLASS ACTION COMPLAINT
v.	)	JURY TRIAL DEMANDED
P.F. CHANGS CHINA BISTRO, INC.,	)	
Defendant.	)	

Plaintiff Daniel Lovell on behalf of a class of similarly situated people (further defined below) alleges the following upon personal knowledge as to himself and his own acts and as to all other matters upon information and belief, based upon, among other things, his attorneys' investigation.

I. INTRODUCTION

1. A data breach is not an act of God. It is, almost always, the predictable and preventable result of one or more security failures by the targeted company. According to a 2014 report by the Online Trust Alliance—an industry group of leading cybersecurity experts—89% of data breaches in 2013 were preventable. Similarly, Verizon Enterprise Solution's 2014 Data Breach Investigations Report—which examined over 63,000 security incidents with the assistance of dozens of industry and government stakeholders—found that "nearly every incident involve[d] some element of human error." The Verizon report found that 92% of all attacks fell into one of nine predictable (and, thus, preventable) patterns.

2. Defendant P.F. Chang's China Bistro ("P.F. Chang's" or the "Company") failed to prevent a significant data breach that compromised its customers' personal financial data (the

"Breach"). As a result of P.F. Chang's lapses, criminal hackers were able to obtain access to credit and debit card data from customers who used their payment cards at P.F. Chang's between September 18, 2013 and June 11, 2014 (the "Relevant Period"; those who used a credit or debit card at a U.S.-based P.F. Chang's within the Relevant Period are members of the "Class").

3. During the Relevant Period, P.F. Chang's failed to disclose to the Class that its subpar security systems placed their financial data at risk. Had Class members received full disclosure of the security risks to which P.F. Chang's was exposing them, they would have paid less for their meals or not purchased them at all. Now that the Breach has occurred, Class members have been further damaged by the need to take affirmative measures to protect against fraudulent charges and other acts of identity theft.

II. PARTIES

4. Plaintiff Daniel Lovell is, and at all relevant times was, a resident of Olympia, Washington. On February 19, 2014, February 20, 2014, and May 6, 2014, Mr. Lovell ate at a P.F. Chang's location in Seattle, Washington and paid with a credit card each time. In total, Mr. Lovell spent $53.67 at P.F. Chang's over the course of his three visits. Upon information and belief, Mr. Lovell's credit card data was stolen as part of the Breach. As a result of the breach, Mr. Lovell is now forced to monitor his financial accounts for fraudulent charges and other indications of identity theft. Had Mr. Lovell known that P.F. Chang's did not abide by industry-standard cybersecurity practices, he would have paid less for his meal or not eaten at P.F. Chang's at all.

5. Defendant P.F. Chang's China Bistro is a Delaware corporation with corporate headquarters in Scottsdale, Arizona. P.F. Chang's is a wholly owned subsidiary of Centerbridge

Partners, a New-York-based private equity firm. P.F. Chang's does not franchise domestically in the United States. It directly owns all of its U.S. restaurants.

III. JURISDICTION AND VENUE

6. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because members of the proposed Class are citizens of states different from P.F. Chang's home states, and the aggregate amount in controversy exceeds $5,000,000.

7. P.F. Chang's is subject to personal jurisdiction in this Court because it operates multiple locations in Washington and Plaintiff's claims arise, in part, from payments that he made to P.F. Chang's in Seattle, Washington.

8. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a) because a substantial part of the events or omissions giving rise to these claims occurred in this district, and P.F. Chang's has caused harm to class members residing in this District.

IV. SUBSTANTIVE ALLEGATIONS

A. P.F. Chang's Customer Data Was Stolen

9. On June 10, 2014, Brian Krebs—an independent investigative reporter widely considered to be a leading cybersecurity expert—reported that "thousands of newly-stolen credit and debit cards went up for sale on rescator[.]so, an underground store best known for selling tens of millions of cards stolen in the Target breach." Krebs contacted several banks who stated that the cards offered for sale had been "previously issued to customers, and found that all had been used at P.F. Chang's locations[.]" P.F. Chang's stated, at the time, that it had not yet been able to confirm a breach but was "in communications with law enforcement authorities and banks to investigate the source."

10. On June 13, 2014, P.F. Chang's confirmed the Breach and issued the following statement:

> On Tuesday, June 10, P.F. Chang's learned of a security compromise that involves credit and debit card data reportedly stolen from some of our restaurants. Immediately, we initiated an investigation with the United States Secret Service and a team of third-party forensics experts to understand the nature and scope of the incident, and while the investigation is still ongoing, we have concluded that data has been compromised.
>
> At P.F. Chang's, the safety and security of our guests' payment information is a top priority. Therefore, we have moved to a manual credit card imprinting system for all P.F. Chang's China Bistro branded restaurants located in the continental United States. This ensures our guests can still use their credit and debit cards safely in our restaurants as our investigation continues.
>
> We have also established a dedicated public website, pfchangs.com/security, for guests to receive updates and answers to their questions.
>
> Because we are still in the preliminary stages of our investigation, we encourage our guests to be vigilant about checking their credit card and bank statements. Any suspected fraudulent activity should be immediately reported to their card company.
>
> We sincerely regret the inconvenience and concern this may cause for our guests.

11. A spokesperson for P.F. Chang's stated further that "all domestic P.F. Chang's branded restaurants in the Continental U.S. will be retaining the carbon copies [of manually imprinted cards]. P.F. Chang's is also deploying dial-up card readers to restaurants that will be plugged in via the PSTN fax line and used to process the slips."

12. On June 18, 2014, Krebs reported that Visa had sent a Compromised Account Management System ("CAMS") alert on June 17, 2014 to at least one bank stating that the bank had "many hundreds of cards exposed in a recent breach that dated back to Sept. 18, 2013. That bank had purchased more than a dozen cards sold from an underground store [that had] been exclusively selling cards stolen in the P.F. Chang's break-in, and every one of those cards was listed on the June 17 CAMS alert from Visa."

13. On July 1, 2014, P.F. Chang's issued the following statement and Frequently Asked Questions (FAQ) section:

STATEMENT FROM RICK FEDERICO
CEO OF P.F. CHANG'S

JULY 1, 2014

We continue to make progress in our investigation into the recent security compromise that affected P.F. Chang's.

The following frequently asked questions have been updated to address many of the questions or concerns you may have.

We will continue sharing important details once they have been confirmed by a team of third-party forensic experts. This website remains the best source of information on the investigation into the compromise and our ongoing response.

We look forward to welcoming you at our restaurants and appreciate your patience as the investigation continues.

1. WHAT HAPPENED?

On Tuesday, June 10, P.F. Chang's learned of a security compromise that involves credit and debit card data reportedly stolen from some of our restaurants. Immediately, we initiated an investigation with the United States Secret Service and a team of third-party forensics experts to understand the nature and scope of the incident, and have concluded that data has been compromised.

2. WHEN DID P.F. CHANG'S DISCOVER THIS INCIDENT?

The United States Secret Services alerted P.F. Chang's to this incident on June 10, 2014.

3. WHEN DID THIS INCIDENT START?

We are coordinating with the United States Secret Service on an investigation to determine when the incident started and what information is involved. To assist with these efforts, P.F. Chang's retained specialized data privacy counsel and forensics experts who are actively assisting in the investigation.

4. WHY IS THE INVESTIGATION TAKING SO LONG?

The security compromise was part of a highly sophisticated criminal operation that is being investigated by both the United States Secret Service and a team of third-party forensic experts. An investigation of this nature takes time, and while we would like to be in a position to provide further information, we can only share details that have been confirmed by the investigators.

5. WHAT INFORMATION WAS EXPOSED?

According to the United States Secret Service, credit card and debit card numbers that have been used at P.F. Chang's are involved.

6. WHAT ACTION SHOULD I TAKE?

If you suspect fraudulent activity on your credit card or debit card, we urge you to report this suspected fraudulent activity to your card company or issuing bank.

7. WHAT ACTION IS P.F. CHANG'S TAKING IN RESPONSE TO THIS INCIDENT?

P.F. Chang's continues to work with a team of third-party forensic experts to investigate this incident. P.F. Chang's is also cooperating with the United States Secret Service as they investigate. Once our investigation has determined the scope of the compromise, we will provide that information on this website.

8. IS IT SAFE FOR CUSTOMERS TO USE THEIR CREDIT CARD/DEBIT CARD?

Yes. It is safe for our guests to use their credit and debit cards in our restaurants. We are using encryption-enabled terminals to securely process credit and debit card information.

9. WHY DID YOU DECIDE TO USE MANUAL CREDIT CARD IMPRINTING DEVICES? HOW LONG WILL YOU HOLD ONTO MY SLIP FOR?

When we became aware of the security compromise, our first priority was to ensure the safety and security of our guests' payment information in our restaurants. The fastest alternative was to transition to manual imprinting devices (a.k.a. "knuckle busters") to safely process credit and debit card payments at all P.F. Chang's China Bistro branded restaurants in the continental U.S. P.F. Chang's is handling the storage and destruction of these slips according to the data protection processes required by the credit and debit card companies.

We have recently deployed additional encryption-enabled terminals to improve speed and automation in an effort to phase out the use of the "knuckle busters."

10. IF YOU ARE USING MANUAL IMPRINTING DEVICES, WHY DOES MY RECEIPT LOOK LIKE IT WAS PROCESSED ELECTRONICALLY?

> All P.F. Chang's China Bistro branded restaurants in the continental U.S. were provided with an encryption-enabled terminal to securely process credit and debit card information. Over the last week, we have deployed additional terminals to our restaurants, which has helped the speed and automation of our transactions. It has also allowed our restaurants to begin phasing out the manual credit card imprinting. In the near future, we will complete the deployment of new hardware and begin the transition back to our standard card processing system.
>
> 11. WILL P.F. CHANG'S CONTACT ME IF MY CREDIT CARD WAS INVOLVED?
>
> We are continuing to work closely with the third party forensic team and will provide information to the credit card companies to assist with efforts to identify the affected cards. The card companies can then provide this information to the issuing banks, who have the best means of directly contacting their affected credit and debit card holders. We encourage all of our guests to continue monitoring their accounts and to report any suspected fraudulent activity to their card company or issuing bank.
>
> Once the investigation has determined the scope of the compromise, we will provide that information on our dedicated website pfchangs.com/security. Please check this website for updates.
>
> 12. WHERE SHOULD I GO FOR UPDATES?
>
> We encourage you to check this website for updates. If you have additional questions, you may also call 1-877-412-7152.

B. P.F. Chang's Likely Could Have Prevented the Breach

14. For several reasons, it is highly likely that—as in most data breaches—incompetence and negligence by the target company, P.F. Chang's, caused the Breach.

15. First, the widely reported breach of Target Corporation should have put P.F. Chang's on notice to ensure that its own systems were not vulnerable to a similar attack. The Target breach was first reported in December 2013. The Target breach affected tens of millions of people, was the subject of a Congressional investigation, led to dozens of lawsuits and resulted in the resignations of Target's CEO and its Chief Information Officer.

16. The evidence suggests that the P.F. Chang's Breach was committed by the same people who committed the Target breach and that they used the same or similar methods to attack P.F. Chang's. As noted above, the stolen P.F. Chang's cards were advertised on the same underground website that sold many of the cards that were stolen in the Target breach. Moreover, it has been reported that the Target breach was accomplished by installing malicious software ("malware") known as BlackPOS on Target's point-of-sale terminals. It seems likely that the P.F. Chang's attack also targeted point-of-sale terminals because the Company's response was to stop swiping cards using its point-of-sale terminals. Matthew J. Schwartz, a cybersecurity expert and reporter for InformationWeek, echoed this conclusion in a June 17, 2014 article, writing that "[g]iven the Rescator connection detailed above, it's possible that P.F. Chang's was [like Target] also compromised using POS malware. P.F. Chang's investigators - based either on early findings or else simply prudence - seem to have come to a similar conclusion, since the restaurant chain last week stopped swiping cards using its POS terminals."

17. In a June 13, 2014 story, eWeek (a leading information technology website) reported that "Philip Casesa, director of IT/service operations for security education group (ISC)2, told eWEEK that P.F. Chang's security compromise appears to follow the same approach that attackers leveraged in the big Target breach, in which point-of-sale (POS) machines with traditionally weak security were targeted." "Large retailers maintain centralized connections to these machines for updating, and an attacker can exploit that to distribute malware efficiently and collect large swaths of magnetic stripe data from the cards," Casesa said. "Without proper detection of this malware on the retailer's part, these breaches can run almost unfettered until the attackers have enough or their exploit window is somehow closed."

18. Second, the length of time that P.F. Chang's security was compromised strongly suggests that the Company was failing to comply with the Payment Card Industry Data Security Standard ("PCI DSS"). PCI DSS is an industry-standard information-security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and point-of-sale cards. Among other policies and procedures, PCI DSS Requirement 10 requires organizations to "Regularly Monitor and Test Networks." This includes establishing audit logs that track access to all systems and conducting a regular review of those logs. Requirement 10.6 states that organizations must "Review logs and security events for all system components to identify anomalies or suspicious activities" and states that "Many breaches occur over days or months before being detected. Checking logs daily minimizes the amount of time and exposure of a potential breach."

19. PCI DSS Requirement 10.6.1 elaborates on the logs that should be reviewed daily: "All security events; Logs of all system components that store, process, or transmit [cardholder data] and/or [sensitive authentication data], or that could impact the security of [cardholder data] and/or [sensitive authentication data]; Logs of all critical system components; Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)."

20. P.F. Chang's failure to detect the Breach for almost nine months suggests that it was failing to implement the daily log monitoring requirements of PCI DSS. In a June 12, 2014 statement, John Harmon, the Principal Consultant of Sword & Shield Enterprise Security stated, with respect to the P.F. Chang's breach, that "Following the PCI DSS requirements, particularly the requirement for daily log monitoring will limit your breach to one or two days, not months."

21. Third, there is significant evidence that P.F. Chang's was using outdated point-of-sale software. P.F. Chang's uses the Aloha brand of point-of-sale terminals. A July 18, 2014 story by ComputerWorld reported that "Matt Oh, a senior malware researcher with HP, recently bought a single Aloha point-of-sale terminal" and found "an eye-opening mix of default passwords, at least one security flaw and a leftover database containing the names, addresses, Social Security numbers and phone numbers of employees who had access to the system. His findings have received a fair amount of attention due to the role of such systems in high-profile data breaches at retailers including Target, Neiman Marcus and Michaels." According to the story, Oh "also found a memory-related problem known as a 'heap overflow' within a component called the Aloha Durable Messaging Service, which shuttles information between front-end and back-end systems. If exploited, the heap overflow 'could provide an attacker with full system level control of the target system'. . . ."

22. According to the ComputerWorld story, "POS systems are generally supposed to be segregated from the Internet. But restaurants often make configuration errors[.]" P.F. Chang's appears to have deliberately allowed remote access to its Aloha point-of-sale terminals. According to a "P.F. Changs Case Study" published by HotSchedules, Inc., "[a]long with the P.F. Chang's IT team, HotSchedules helped to develop a custom interface for [P.F. Chang's] Aloha POS." Using that HotSchedules software, managers can access the HotSchedules Manager portal, "anywhere, anytime, easily and securely over the web." Moreover, "staff schedules export nightly to the Aloha POS[.]" The ComputerWorld story quoted Joseph Snell, the CEO of a restaurant payment company called Viableware, who stated that P.F. Chang's used the Aloha software and that "[t]hey had a hole in their armor, and an arrow went right through it."

C. Plaintiff and the Class Have Been Harmed

23. During the Relevant Period, P.F. Chang's failed to disclose to the Class any of the security weaknesses described above. Had Class members received full disclosure of the security risks to which P.F. Chang's was exposing them, they would have paid less for their meals or not purchased them at all.

24. Plaintiff and the Class have been further harmed because, as a result of the Breach, cyber-criminals now possess their personal financial information. While credit card companies offer protection against unauthorized charges, the process is long, costly, and frustrating. Physical cards must be replaced, credit card information must be updated on all automatic payment accounts, and victims must add themselves to credit fraud watch lists, which substantially impairs victims' ability to obtain additional credit. Information about Plaintiff and the other Class Members may also be used to harass or stalk them.

25. Plaintiff brings this action on behalf of himself and the following Class, pursuant to Rules 23(a) and (b)(3) of the Federal Rules of Civil Procedure:

> All persons in the United States who used a debit or credit card at a P.F. Chang's restaurant between September 18, 2013 and June 11, 2014.

26. The Class excludes the officers and directors, and current or former employees, as well as immediate family members thereof, of P.F. Chang's and its parents, subsidiaries, and affiliates.

27. Plaintiff reserves the right to amend the definition of this proposed Class, including by adding subclasses.

28. The Class is so numerous that joinder of all members is impracticable. P.F. Chang's has over 210 full service restaurants in the United States and the Breach lasted for almost nine months. It is almost certain that thousands of cards were compromised.

29. There are questions of fact or law common to the Class. These questions include, but are not limited to:

a. Whether P.F. Chang's had a duty to disclose failures to comply with industry-standard cybersecurity practices;

b. Whether P.F. Chang's complied with industry-standard cybersecurity practices;

c. Whether P.F. Chang's concealed its noncompliance with industry-standard cybersecurity practices from its customers; and

d. Whether P.F. Chang's failure to comply with industry-standard cybersecurity practices caused the Breach.

30. Plaintiff's claims are typical of the Class and Plaintiff is not subject to any unique defenses.

31. Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff's interests do not conflict with the interests of the Class. Plaintiff has retained competent counsel experienced in class action litigation of this type. Plaintiff's counsel will fairly and adequately protect the interests of the Class.

32. Certification is appropriate under Federal Rule of Civil Procedure 23(b)(3) because questions of law or fact common to the Class predominate over any questions affecting only individual members.

33. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Individual lawsuits are economically infeasible and procedurally impracticable.

34. Plaintiff knows of no difficulty to be encountered in the management of this case that would preclude its maintenance as a class action.

V. CLAIMS ALLEGED AND RELIEF SOUGHT

A. Claims Asserted By The Class

COUNT 1
Negligence

35. Plaintiff and the Class incorporate by reference the foregoing allegations as though fully set forth herein.

36. P.F. Chang's owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting their personal and financial information in its possession from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing P.F. Chang's security systems to ensure that Plaintiff and Class member's financial information was adequately secured and protected. P.F. Chang's further had a duty to implement processes that would detect a breach of its security system in a timely manner.

37. P.F. Chang's breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff and Class members' financial data in its possession by failing to adopt, implement, and maintain adequate security measures to safeguard their data; failing to adequately monitor the security of its point-of-sale systems; allowing unauthorized access to Plaintiff and Class members' data; and failing to recognize in a timely manner that its security had been breached.

38. P.F. Chang's failures to comply with industry standards, such as PCI DSS are evidence of P.F. Chang's negligence in failing to exercise reasonable care in safeguarding and protecting the customer data in its possession.

39. But for P.F. Chang's wrongful and negligent breach of its duties owed to Plaintiff and other Class members, their financial data would not have been compromised.

40. The injury and harm suffered by Plaintiff and Class members was the reasonably foreseeable result of P.F. Chang's failure to exercise reasonable care in safeguarding and protecting the financial data collected from customers. P.F. Chang's knew or should have known that its systems and technologies for processing and securing customers' data had security vulnerabilities.

COUNT 2
Breach Of Implied Contract

41. Plaintiff and the Class incorporate by reference the foregoing allegations as though fully set forth herein.

42. When they confided their private and confidential debit card and credit card information to Defendant in order to make purchases at Defendant's restaurants, Plaintiff and Class members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect all such information.

43. Plaintiff and Class members would not have entrusted their private and confidential financial and personal information to Defendant in the absence of such an implied contract with Defendant.

44. Defendant breached the implied contracts made with Plaintiff and Class members by failing to safeguard such information.

45. The damages sustained by Plaintiff and Class members as described above were the direct and proximate result of Defendant's breaches of these implied contracts.

COUNT 3
Breach of Fiduciary Duty

46. Plaintiff and the Class incorporate by reference the foregoing allegations as though fully set forth herein.

47. Plaintiff and Class members entrusted private and confidential financial and personal information to the Defendant at Defendant's request and placed trust and confidence in the Defendant in order to make payments to Defendant.

48. Defendant had the benefit of a disparity of position and control and Plaintiff and Class members placed trust and confidence in Defendant.

49. Defendant had a duty to maintain the confidentiality of the private and confidential financial and personal information, to safeguard and protect it from misuse by unauthorized persons.

50. Defendant breached its duty by failing to take necessary measures to maintain the confidentiality of Plaintiff's and Class members' private and confidential financial and personal information and to safeguard and protect it from misuse by unauthorized persons.

51. The damages sustained by Plaintiff and Class members as described above were the direct and proximate result of Defendant's breach of its duty of a confidential relationship.

COUNT 4
Strict Liability

52. Plaintiff and the Class incorporate by reference the foregoing allegations as though fully set forth herein.

53. Defendant failed adequately to safeguard the private and confidential financial and personal information of their customers entrusted to it in the course of purchases made with debit cards and credit cards during the Relevant Period.

54. Payment by debit or credit card increasingly is a necessity for consumers. Lack of such means of payment increasingly limits their purchase options and bargaining power. Restaurants such as P.F. Chang's are eager to accept credit cards—and pay credit card

companies handsomely for that privilege—because customers using credit cards spend more money than those paying with cash.

55. Increasing reliance on electronic means of payment and other recording of personal identity and financial data has left consumers increasingly susceptible to personal data and identity theft, the adverse consequences of which also are of increasing severity.

56. Safeguarding private and confidential data of others in their possession is solely within the control of the recipients of that data, who are best able to distribute the cost of maintaining the security of that data and the consequences of the breach of such security.

57. Plaintiff and Class members confided and entrusted their private and confidential financial and personal information to Defendant solely for the purpose of effectuating payment for purchases made from Defendant and with the expectation that Defendant would strictly maintain the confidentiality of the information and safeguard it from theft or misuse.

58. Plaintiff and Class members did not contribute in any way to the breach of Defendant's information technology systems or the compromise or theft of their private and confidential financial and personal data. Accordingly, Defendant should be held strictly liable for the loss and damage suffered by Plaintiff and Class members resulting from Defendant's failure to safeguard and maintain the confidentiality of their financial and personal data.

COUNT 5
Negligent Misrepresentation

59. Plaintiff and the Class incorporate by reference the foregoing allegations as though fully set forth herein.

60. P.F. Chang's had special knowledge of the methods and flaws in the methods by which it secured customer payments. Plaintiff and the Class did not have access to that information. This information was material to Plaintiff and Class members' decision to purchase

their meals at P.F. Chang's. Therefore, P.F. Chang's had a duty to disclose flaws in its security methods.

61. P.F. Chang's did not disclose to Plaintiff or to any Class member that P.F. Chang's did not abide by industry-standard cybersecurity practices—including by failing to conduct daily log monitoring—and had other deficiencies in its cybersecurity.

62. Plaintiff and the Class justifiably relied on this omission, meaning that, under conditions of full disclosure, they would have paid less for their meals or would not have purchased their meals from P.F. Chang's at all.

COUNT 6
Arizona Deceptive Trade Practices Act

63. Plaintiff and the Class incorporate by reference the foregoing allegations as though fully set forth herein.

64. Plaintiff, the Class and P.F. Chang's are "persons" within the meaning of Ariz. Rev. Stat. § 44-1521. The goods and services provided by P.F. Chang's to Plaintiff and the Class are "merchandise" within the meaning of Ariz. Rev. Stat. § 44-1521.

65. Plaintiff and the Class were injured by P.F. Chang's employment of deceptive acts or practices in connection with the sale of merchandise, including, among other things, uniformly failing to disclose its noncompliance with industry-standard cybersecurity practices.

66. As a direct and proximate result of P.F. Chang's deceptive acts and practices, Plaintiff and the Class overpaid for the goods and services that they received from P.F. Chang's and have been damaged thereby.

VI. RELIEF REQUESTED

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully requests that the Court enter judgment in his favor as follows:

A. Certify this matter as a class action, appoint Plaintiff's attorneys as class counsel, and issue notice to the Class;

B. Enter judgment in favor of Plaintiff and the Class against P.F. Chang's;

C. Award to Plaintiff and Class members actual, statutory, and punitive damages;

D. Award appropriate pre- and post-judgment interest;

E. Grant an award of reasonable attorney's fees and other litigation costs reasonably incurred, including expert witness fees; and

F. Award any and all other relief to which Plaintiff and the Class may be entitled.

VII. JURY DEMAND

Plaintiff demands a trial by jury on all claims so triable.

Dated: July 30, 2014

Respectfully submitted,

BLOCK & LEVITON LLP

By: /s/ Jason M. Leviton

Jason M. Leviton (WA #34106)
Whitney E. Street
Joel A. Fleming
Block & Leviton LLP
155 Federal Street, Suite 1303
Boston, Massachusetts 02110
Tel: (617) 398-5600
Fax: (617) 507-6020
Jason@blockesq.com
Whitney@blockesq.com
Joel@blockesq.com

Counsel for Plaintiff